PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+"controlling network access" SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Published before September 2003
Terms used **controlling network access**

Found **2** of **146,187**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 2 of 2

Relevance scale

1 Linux System Administration: Maximizing System Security: Part 2
February 1996 **Linux Journal**
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(18.53 KB) Additional Information: full citation, index terms

2 Security issues on the internet
Carl Stephen Guynes, Richard G. Vedder, Michael T. Vanecek
April 1997 **ACM SIGSAC Review**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(380.62 KB) Additional Information: full citation, abstract, references, citings, index terms

The Internet is a collection of networks originally paid for by the U.S. Department of Defense. Its purpose was to provide a communications infrastructure more resilient to attack than the public communications channels in the event of war. When research became a priority in the 1960s and 1970s, money was given to the National Science Foundation, which became the de facto administrator of the network. The NSF ran the primary arteries of the Internet until the late 1980s. A substantial amount of ...

Results 1 - 2 of 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL
USPTO
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+challenge-response; +network +access; +symmetric +secret
SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Published before September 2003
Terms used
challenge response; network access; symmetric secret

Found **19** of **146,187**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 19 of 19

Relevance scale

1 Cryptographic security Techniques for wireless networks

Danai Patiyoot, S. J. Shepherd
April 1999 **ACM SIGOPS Operating Systems Review**, Volume 33 Issue 2
Publisher: ACM Press
Full text available: pdf(1.12 MB) Additional Information: full citation, abstract, index terms

This paper deals with security techniques for wireless Networks. The work presented is based on a review of literature regarding current and future wireless security networks systems. The aspects discussed in this paper included the choices of cryptographic algorithms such as protocols for key management and authentication. Various conclusions are drawn from existing security networks and proposed in new wireless ATM network security. Also a proposal for future research into security techniques ...

Keywords: cryptographic, security, wireless

2 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3
Publisher: ACM Press
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

3 ID-based secret-key cryptography

Marc Joye, Sung-Ming Yen
October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4
Publisher: ACM Press
Full text available: pdf(513.15 KB) Additional Information: full citation, abstract, citings, index terms

This paper introduces *ID-based secret-key cryptography,* in which secret keys are privately and uniquely binded to an identity. This enables to extend public-key cryptography features at the high throughput rate of secret-key cryptography. As applications, efficient login protocols, an enhanced version of Kerberos, and an ID-based MAC algorithm are presented.ID-based systems were initially developed in the context of public-key cryptography by removing the need of explicit public keys. The ...

Keywords: ID-based systems, Kerberos, MACs, authentication protocols, one-time passwords, secret-key cryptography

4 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent
June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

5 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

6 Computer security: Proxy-based security protocols in networked mobile devices

M. Burnside, D. Clarke, T. Mills, A. Maywah, S. Devadas, R. Rivest
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing SAC '02**
Publisher: ACM Press
Full text available: pdf(765.09 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe a resource discovery and communication system designed for security and privacy. All objects in the system, e.g., appliances, wearable gadgets, software agents, and users have associated trusted software proxies that either run on the appliance hardware or on a trusted computer. We describe how security and privacy are enforced using two separate protocols: a protocol for secure device-to-proxy communication, and a protocol for secure proxy-to-proxy communication. Using two separate ...

Keywords: authorization, certificate, certificate chain, certificate chain discovery, mobile device, pervasive, protocol, proxy, security, ubiquitous, wireless

7 Security & transport: Mobility helps security in ad hoc networks

Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttyán
June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing MobiHoc '03**
Publisher: ACM Press
Full text available: pdf(228.73 KB) Additional Information: full citation, abstract, references, citings, index terms

Contrary to the common belief that mobility makes security more difficult to achieve, we show that node mobility can, in fact, be useful to provide security in ad hoc networks. We propose a technique in which security associations between nodes are established, when they are in the vicinity of each other, by exchanging appropriate cryptographic material. We show that this technique is generic, by explaining its application to fully self-organized ad hoc networks and to ad hoc networks placed und ...

Keywords: ad hoc networks, mobility, security associations

8 Unlinkable serial transactions: protocols and applications

Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press

Full text available: pdf(184.87 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

9 Verifying security protocols as planning in logic programming

Luigia Carlucci Aiello, Fabio Massacci
October 2001 **ACM Transactions on Computational Logic (TOCL)**, Volume 2 Issue 4
Publisher: ACM Press

Full text available: pdf(305.94 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We illustrate *ALSP* (Action Language for Security Protocol), a declarative executable specification language for planning attacks to security protocols. *ALSP* is based on logic programming with negation as failure, and with stable model semantics. In *ALSP* we can give a declarative specification of a protocol with the natural semantics of send and receive actions which can be performed in parallel. By viewing a protocol trace as a plan to a ...

Keywords: AI planning, logic programming, security protocols, specification language

10 Internet security standards: past, present, and future

Stephen Kent
June 1994 **StandardView**, Volume 2 Issue 2
Publisher: ACM Press

Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings, index terms

11 Security protocol for IEEE 802.11 wireless local area network

Se Hyun Park, Aura Ganz, Zvi Ganz
September 1998 **Mobile Networks and Applications**, Volume 3 Issue 3
Publisher: Kluwer Academic Publishers

Full text available: pdf(263.66 KB) Additional Information: full citation, abstract, references, citings, index terms, review

As Wireless Local Area Networks (WLANs) are rapidly deployed to expand the field of wireless products, the provision of authentication and privacy of the information transfer will be mandatory. These functions need to take into account the inherent limitations of the WLAN medium such as limited bandwidth, noisy wireless channel and limited computational power. Moreover, some of the IEEE 802.11 WLAN characteristics such as the use of a point coordinator and the polling based Point Coordinati ...

12

A security architecture for fault-tolerant systems
Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

13 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press
Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

14 NTP retrospective: A brief history of NTP time: memoirs of an Internet timekeeper
David L. Mills
April 2003 **ACM SIGCOMM Computer Communication Review**, Volume 33 Issue 2
Publisher: ACM Press
Full text available: pdf(185.93 KB) Additional Information: full citation, abstract, references, citings

This paper traces the origins and evolution of the Network Time Protocol (NTP) over two decades of continuous operation. The technology has been continuously improved from hundreds of milliseconds in the rowdy Internet of the early 1980s to tens of nanoseconds in the Internet of the new century. It includes a blend of history lessons, technology milestones and series of experiments that shape, define and record the early history of the Internet and NTP.This narrative is decidedly personal, since ...

Keywords: algorithmic memoirs, computer network, technical history, time synchronization

15 Revokable and versatile electronic money (extended abstract)
Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security CCS '96**
Publisher: ACM Press
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

16 Identification control: Secure object identification: or: solving the Chess Grandmaster Problem
Ammar Alkassar, Christian Stüble, Ahmad-Reza Sadeghi
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(782.85 KB) Additional Information: full citation, abstract, references

Many applications of cryptographic identification protocols are vulnerable against physical

adversaries who perform real time attacks. For instance, when identifying a physical object like an automated teller machine, common identification schemes can be bypassed by faithfully relaying all messages between the communicating participants. This attack is known as *mafia fraud*.The Probabilistic Channel Hopping (PCH) system we introduce in this paper, solves this problem by hiding the conversa ...

Keywords: Chessmaster Problem, fake equipment, identification, mafia fraud

17 Strength of two data encryption standard implementations under timing attacks

Alejandro Hevia, Marcos Kiwi

November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosys-tems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

18 Comparing lower bounds on messages and rounds for two classes of key establishment protocols

Anish Mathuria

October 1998 **ACM SIGCOMM Computer Communication Review**, Volume 28 Issue 5

Publisher: ACM Press

Full text available: pdf(532.06 KB) Additional Information: full citation, abstract, index terms

An important requirement in designing protocols for key establishment is to provide assurance to protocol participants that a session key is fresh. This paper compares lower bounds on messages and rounds for two classes of protocols based on fundamentally different methods for achieving session key freshness.

19 Internet printing protocol (IPP) encoding and transport

Carl Kugler, Harry Lewis

December 1998 **StandardView**, Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(399.88 KB) Additional Information: full citation, references

Results 1 - 19 of 19

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1683	713/168.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:39
L2	576	726/2.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:39
L3	634	726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:47
L4	3995	public adj5 secret	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:48
L5	2354	private adj5 secret	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:48
L6	395	l4 same l5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:49
L7	48	l6 same symmetric	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:52
L8	17	l7 same authenticat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 13:56
L9	12	l7 and (challenge near9 response)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 14:02

EAST Search History

L10	41	l6 and (challenge near9 response)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 14:02
L11	28	l10 and (control$4 near5 access$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 14:03
L12	28	l11 and authenticat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/22 14:03